Die neue Verordnung der EU zur Künstlichen Intelligenz

Hilgendorf / Roth-Isigkeit

2023
ISBN 978-3-406-79682-1
C.H.BECK

umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Da einer zuverlässigen Remote-Beobachtung des Systems rechtliche, aber auch tatsächliche Gründe entgegenstehen können, ist es sinnvoll, **Nutzerbeschwerdemechanismen** vorzuhalten, die eine effektive Informationsquelle sein können.[65] 55

IX. Haftungsrechtliche Dimension der verschiedenen Pflichten

Nach offizieller Leseart enthält die Verordnung keine Haftungsregeln.[66] Das Haftungsrecht soll stattdessen einem zweiten KI-spezifischen Gesetz vorbehalten bleiben, das nun in Form eines KIHaft-RL-E (→ § 10 Rn. 81 ff.) vorliegt. Freilich kann nicht davon die Rede sein, der KI-VO-E habe keine haftungsrechtliche Dimension – im Gegenteil:[67] Im deutschen Deliktsrecht wirken sich die oben beschriebenen Verhaltenspflichten aufseiten der Adressaten *erstens* über § 823 Abs. 2 BGB aus. Denn die Regeln unionaler Verordnungen qualifizieren bei unmittelbarer Wirkung zum Bürger als **Schutzgesetze;**[68] dies nicht zuletzt wegen der Haltung des EuGH, die „Durchsetzungskraft" von Unionsrecht werde durch eine zivilrechtliche Absicherung der Pflichten erhöht.[69] Praktisch kann der KI-VO-E eine Erweiterung des Schadensersatzrechts bewirken: Während der Rückruf bereits vermarkteter Produkte nicht zum deliktsrechtlichen Pflichteninhalt zählt, könnte man dies nun wegen den von der KI-VO-E festgeschriebenen Rücknahme- und Rückrufpflichten anders sehen.[70] Darüber hinaus erfahren primäre Vermögensinteressen über § 823 Abs. 2 BGB iVm den Geboten und Verboten des K-VO-E einen vorerst direkten Schutz.[71] *Zweitens* lassen sich die in der Verordnung niedergelegten Verhaltensanforderungen – vor allem jene der Art. 16 ff. KI-VO-E und die produktsicherheitsrechtlich relevanten Regeln – als Konkretisierungstatbestände für allgemeine **Verkehrssicherungspflichten** einordnen. *Drittens* kann den Anforderungen des KI-VO-E mittelbar auch eine Bedeutung für das Pflichtenprogramm des Herstellers entnommen werden.[72] 56

Der KI-VO-E in der vorliegenden Form kommt jedoch nicht nur im Deliktsrecht eine Bedeutung zu. Auch im vertraglichen Haftungsrecht sind die harmonisierten Verhaltensanforderungen zu berücksichtigen. Die Pflichten eines Schuldners folgen aus dem **vertraglichen Pflichtenkatalog** (§ 241 BGB) und aus der Natur des Schuldverhältnisses. Teilweise konkretisiert das Gesetz diese Pflichten; ganz überwiegend sind sie jedoch schrittweise von der Rechtsprechung – unter Berücksichtigung der Lebensbezüge, wozu auch Branchenstandards gehören – entwickelt worden.[73] Die von dem KI-VO-E formulierten Standards bestimmen den Erwartungshorizont des Vertragspartners, indem er berechtigterweise darauf vertrauen darf, dass sein Schuldner die KI-basierten Systeme auf eine Weise einrichtet und einsetzt, die den Anforderungen des KI-VO-E genügen. Dieser berechtigten Gläubigererwartung kann nur Genüge getan werden, wenn eine Missachtung der Standards auch auf vertraglicher Ebene haftungsrechtliche Konsequenzen zeitigt. Eine fehlende Konformität des KI-Systems mit dem KI-VO-E kann sich deswegen zum einen über das allgemeine 57

[65] Ähnl. Wiebe BB 2022, 899 (904).
[66] S. etwa Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter RDi 2021, 528 Rn. 56; vgl. auch → § 10 Rn. 6.
[67] Spindler CR 2021, 361 Rn. 4; Roos/Weitz MMR 2021, 844 (849 f.), dort auch zur vertragsrechtlichen Dimension des Entwurfs; Geibel GPR 2021, 194 (196), dort auch zur produkthaftungsrechtlichen Bedeutung des Entwurfs; allg. Linardatos GPR 2022, 58 (60); Grützmacher CR 2021, 433 Rn. 36 ff.; wohl skeptisch Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter RDi 2021, 528 Rn. 56. Zur haftungsrechtlichen Bedeutung der Zertifizierungen: Buchner Int. Cybersecur. Law Rev. 2022, 181 (187).
[68] BGHZ 188, 326 Rn. 17; s. auch BGH GRUR 1999, 276 (277); MüKoBGB/Wagner BGB § 823 Rn. 539; Wagner DeliktsR Rn. 225.
[69] EuGH BeckRS 2004, 75459 Rn. 30 f.; EuZW 2001, 715 Rn. 26 ff.
[70] So Grützmacher CR 2021, 433 Rn. 60.
[71] Zu entsprechenden Forderungen bereits Linardatos Autonome und vernetzte Aktanten im Zivilrecht S. 358 bei Fn. 1079.
[72] Grützmacher CR 2021, 433 Rn. 74 mit entsprechenden Beispielen.
[73] Dazu s. auch Linardatos Autonome und vernetzte Aktanten im Zivilrecht § 8 A. IV. 3.

Leistungsstörungsrecht (§§ 280 ff. BGB), zum anderen über gewährleistungsrechtliche Ansprüche (§§ 327 ff., 434 ff. BGB) auswirken.[74]

B. Korrekturmaßnahmen

58 Anbieter von Hochrisikosystemen sind gemäß Art. 21 KI-VO-E nach Inverkehrgabe oder Inbetriebnahme des Systems verpflichtet, rechtlich **nicht akzeptierte Betriebsaktivitäten** und **Systemeigenschaften** zu **korrigieren.** Die Korrekturmaßnahmen bilden das Gegenstück zu den Konformitätsbewertungsschritten, die vor Inverkehrgabe oder Inbetriebnahme zu ergreifen sind. Gerade im Zusammenhang mit KI-Systemen, die sich dynamisch (weiter-)entwickeln und verändern können, können Korrekturmaßnahmen – die Ausnahme des Art. 43 Abs. 4 UAbs. 2 KI-VO-E vorbehalten[75] – notwendig werden, denn es ist nicht auszuschließen, dass sich das System in eine Richtung entwickelt, die von der ursprünglichen Konformitätsbewertung und der CE-Zertifizierung nicht mehr gedeckt ist.

59 Die Korrekturmaßnahmen sind prinzipiell **produktstückspezifisch.** Ist jedoch eine gleichartige Produktreihe auf dem Markt oder wird eine gesamte „Flotte" mit demselben KI-System betrieben, so sind typischerweise für alle Produktstücke entsprechende Korrekturmaßnahmen zu ergreifen, selbst wenn sich der Fehler bisher nur bei einzelnen Systemen oder Einheiten manifestiert hat.[76] Nur dies wird dem Präventionsgedanken des KI-VO-E ausreichend gerecht.

60 Begrifflich ist der Normtext des Art. 21 KI-VO-E zu eng geraten, denn es sind nicht nur Korrekturen im engeren Sinne zu ergreifen, sondern es kommen auch reine **Anpassungen** in Betracht; dies ist zB bei veränderten regulatorischen Rahmenbedingungen der Fall.

I. Voraussetzungen der Pflichtenentstehung

1. Grundlagen

61 Eine Korrekturpflicht entsteht, wenn ein Anbieter „der Auffassung" ist oder „Grund zu der Annahme" hat, ein von ihm verantwortetes Hochrisikosystem weise nicht mehr rechtskonforme Aktivitäten oder Eigenschaften auf. Art. 21 KI-VO-E stellt expressis verbis diese Pflicht nur auf, wenn das betreffende KI-System nicht (mehr) den Anforderungen des KI-VO-E entspricht. Diese sprachliche Verengung kann nicht materiell-rechtlich beachtlich sein. Der Anbieter eines Hochrisikosystems hat selbstverständlich auch in jenen Fällen geeignete Korrekturmaßnahmen zu ergreifen, in denen das System zwar mit dem KI-VO-E konform ist, aber anderen Rechtsakten – etwa der DS-GVO – zuwiderläuft.

62 Unklar ist, was unter „Auffassung" zu verstehen ist und wann ein ausreichender „Grund zu der Annahme" besteht, das System sei womöglich nicht mehr rechtskonform im Verkehr oder im Betrieb. Der Gesetzeswortlaut wird vermutlich dahingehend zu verstehen sein, dass es nicht auf eine präzise Subsumption ankommt und bereits **subjektive Verdachtsmomente** aufseiten der Anbieter zur Reaktion veranlassen sollten. Solche Verdachtsmomente können etwa durch Kunden- und Händlerbeschwerden entstehen, aber auch bei entsprechenden Medienberichten oder Testergebnissen von Verbraucherorganisationen (etwa Stiftung Warentest). Es kommt demnach nicht darauf an, ob die Korrekturmaßnahmen auch objektiv geboten oder erforderlich sind. Indes können sich subjektive und objektive Ebene decken: Wenn nämlich auf öffentlichem Wege dem Anbieter etwaige

[74] Roos/Weitz MMR 2021, 844 (849 f.).
[75] Dazu schon → Rn. 15 ff.
[76] S. die spiegelbildlich geltenden Regeln bei der Konformitätsbewertung → Rn. 12 ff.

Sicherheitsprobleme bekannt werden, dann sind Korrekturen oder Anpassungen nicht nur subjektiv, sondern auch objektiv gesehen notwendig.

Bei entsprechender Ausgestaltung des KI-Systems und im Rahmen des gesetzlich Zulässigen (VO (EU) 2016/679, GeschGehG etc.) ist es denkbar, dass der Anbieter in Echtzeit mit dem Hochrisikosystem verbunden ist und laufend mit Metadaten versorgt wird. Er erfüllt damit seine Pflicht zur Beobachtung nach dem Inverkehrbringen gem. Art. 61 KI-VO-E.[77] Zeigen sich etwaige Anomalien in diesen Datenbeständen, dann kann dies etwaige Prüf- oder Untersuchungspflichten sowie Korrektur- und Anpassungsmaßnahmen bedingen. Die Beobachtungspflicht erstreckt sich hierbei auch auf fremdproduzierte Komponenten.[78] 63

2. (Ungeschriebene) Risikoschwelle?

Art. 21 KI-VO-E begründet eine Pflicht zur Korrektur ausnahmslos, sobald das betreffende KI-System nicht (mehr) den Anforderungen des KI-VO-E entspricht. Eine anbieter- und letztlich auch marktschonende Risikoschwelle scheint nicht vorgesehen zu sein. Demnach könnte man Art. 21 KI-VO-E dahingehend lesen, jede Nichtkonformität sei ein nicht akzeptables Risiko. Da jedoch eine absolute Systemsicherheit und Risikofreiheit nicht verlangt sein kann,[79] besteht auf Anbieterseite nicht die Pflicht, jegliches Restrisiko zu beseitigen.[80] Entsprechend sind nur „erforderliche" Maßnahmen zu ergreifen. Diese Einschränkung betrifft indes nicht den Korrekturanlass, sondern die Korrekturtiefe und den damit verbundenen -aufwand.[81] Folglich hängt die Pflicht, für etwaige Korrekturen tätig zu werden, nicht von der Überschreitung einer Risikoschwelle ab. Jede Konformitätsabweichung verlangt vom Anbieter, zumindest prüfend aktiv zu werden und etwaige Korrekturen auszuloten. Anders als nach bisherigem Deliktsrecht[82] sind **bloße Warnungen nicht mehr ausreichend** (→ § 10 Rn. 50). 64

II. Rechtsfolgen

Auf Rechtsfolgenseite des Art. 21 KI-VO-E gilt, dass die **erforderlichen Korrekturen** zu ergreifen sind, um die Konformität des Systems wieder herzustellen. Ziel ist die **Risikoabwehr.** Korrekturmaßnahmen sind demnach alle Maßnahmen, mit denen den Verordnungsanforderungen wieder entsprochen werden kann. Den Korrekturen zwingend vorgeschaltet sind Prüf-, Untersuchungs- und Testobligationen, denn es besteht – wie eben gesehen – eine Reaktionspflicht des Anbieters bereits bei einem bloßen Verdacht fehlender Konformität. Etwaige Verdachtsmomente lassen sich nur erhärten, wenn die Aktivitäten und Eigenschaften des Systems näher überprüft und festgestellt werden. Zudem ist es kaum möglich, die erforderlichen Korrekturen zu bestimmen, ohne das System zuvor entsprechend durchleuchtet zu haben. 65

[77] S. dazu schon → Rn. 51 ff.
[78] Vgl. grundlegend BGHZ 99, 167 = NJW 1987, 1009.
[79] Nicht nur dem Produktsicherheits-, sondern auch dem Produkthaftungsrecht ist das Erfordernis absoluter Fehlerfreiheit fremd; vgl. hierzu schon Linardatos Autonome und vernetzte Aktanten im Zivilrecht § 8 I. 2.; s. auch BGHZ 80, 186, 190; BGH NJW 2013, 1302; Wagner AcP 217 (2017), 707 (728 f.).
[80] Vgl. auch Art. 9 Abs. 4 S. 2 KI-VO-E, wo vorgeschrieben ist, Anbieter müssten Nutzern etwaige Restrisiken mitteilen. Die Vorschrift ergibt nur Sinn, wenn man ihr implizit die Akzeptanz von Restrisiken entnimmt. Die tschechische EU-Ratspräsidentschaft hat allerdings vorgeschlagen, Art. 9 Abs. 4 S. 2 KI-VO-E zu streichen (vgl. Ratsdok. 11124/22).
[81] S. sogleich noch → Rn. 66 f.
[82] Vgl. BGHZ 179, 157 (160) = NJW 2009, 1080 (1081); BGHZ 80, 186 (191) = NJW 1981, 1603 (1604).

1. Erforderliche Korrekturen

66 Etwaige Korrekturen setzen voraus, dass der verpflichtete Anbieter im Besitz des jeweiligen Hochrisikosystems oder jedenfalls mit diesem datentechnisch verbunden ist, um bspw. ein allfälliges **Softwareupdate** aufzuspielen. Fehlt es am Besitz oder an der Datenverbindung zum System, dann muss der Anbieter auf den Besitzer oder auf sonstige zugriffsbefähigte und -befugte Personen geeignet einwirken, um die entsprechende Korrektur zu veranlassen. Demnach greift der Wortlaut des Art. 21 S. 2 KI-VO-E zu kurz, soweit er dem Anbieter nur die Pflicht auferlegt, Händler, andere Bevollmächtigte und Einführer über die erforderlichen Maßnahmen zu informieren; eine bloße Information genügt ersichtlich nicht.

67 Die Korrekturen sind in einem finanziell angemessenen Rahmen zu erbringen. Art. 21 KI-VO-E hat nicht das Ziel, eine allgemeine Verbesserung des Produktstandards zu bewirken, weil diese Verhaltensincentivierung den Marktkräften vorbehalten ist. Es soll allein die Gesetzeskonformität wiederhergestellt werden, selbst wenn im Übrigen das System unter dem Marktstandard bleibt. Zu erfüllen sind demnach nur **erforderliche** und somit **verhältnismäßige Korrekturen.**[83] Der mit den Korrekturen finanzielle Aufwand hat freilich keine entlastende Bedeutung, sofern die Beachtung dieses Einwands zu Maßnahmen führen würde, die etwaige Gefahren für die menschliche Gesundheit oder andere Rechtsgüter nicht beseitigen. Damit ist indes nicht gemeint, das System müsse nach den Korrekturen absolut fehler- oder risikofrei sein. Entscheidend ist letztlich der „Schutzbedarf" im jeweiligen Handlungsfeld:[84] Anhand von analytisch-statistischen Schadensszenarien werden die möglichen Schäden bestimmt, die vom nicht-konformen System ausgehen können, und anknüpfend daran werden die „erforderlichen" Maßnahmen ergriffen. Praktisches Ziel der Anbieter wird es sein, die Anforderungen der Vermutungsregel gem. Art. 40 KI-VO-E (wieder) zu erreichen.

2. Rücknahme vom Markt oder Rückruf

68 Ist eine Korrektur oder Anpassung mangels Zugriffs- oder Einwirkungsmöglichkeit nicht umsetzbar oder ist sie nicht geeignet, die Konformität des Systems herzustellen, so greift die Pflicht zur Rücknahme vom Markt oder zum Rückruf (Art. 21 KI-VO-E). Gem. Art. 3 Nr. 16 KI-VO-E ist unter einem **Rückruf** jede Maßnahme zu verstehen, „die auf die Rückgabe eines den Nutzern bereits zur Verfügung gestellten KI-Systems an den Anbieter abzielt". Eine **Rücknahme** bezeichnet hingegen jede Maßnahme, mit der verhindert werden soll, dass ein KI-System vertrieben, ausgestellt oder angeboten wird (Art. 3 Nr. 17 KI-VO-E).[85]

69 Begrifflich sind die Termini Rückruf und Rücknahme zu eng geraten; sie stammen aus der Welt verkörperter Produkte. Bei nichtkörperlichen KI-Systemen werden die Rückruf- bzw. Rücknahmepflichten durch **Stilllegungen, Löschungen** oder **Zugriffssperren** verwirklicht.[86]

70 Gem. Art. 21 S. 2 KI-VO-E besteht für den Anbieter eine Pflicht, etwaige Händler, Bevollmächtigte und Einführer über die erforderlichen Maßnahmen zu informieren. Sprachlich ist dies zu kurz gegriffen. Vom Gesetz muss vielmehr gemeint sein, dass die Anbieter auf die betreffenden Marktteilnehmer einwirken, damit diese auch tatsächlich geeignet mitwirken, um einen Rückruf oder eine Rücknahme sicherzustellen, bevor (weite-

[83] Allgemein zum Verhältnismäßigkeitsgrundsatz im Produktsicherheitsrecht s. etwa Klindt ProdSG/Kapoor, ProdSG § 16 Rn. 11.
[84] S. allgemein dazu Zimmer Regulierung von Algorithmen und Künstliche Intelligenz/Poretschkin/Mock/Wrobel S. 175 (191).
[85] Nach dem Kompromissvorschlag der slowenischen Ratspräsidentschaft soll die Rücknahme dahingehend verstanden werden, es seien Maßnahmen gemeint, die das KI-System aus den Lieferketten rausnehmen, vgl. Art. 3 Nr. 17 Ratsdok. 14278/21.
[86] Wiebe BB 2022, 899 (904).

re) Schäden entstehen. Eine bloße Information von einer Rücknahme- oder Rückrufabsicht reicht hingegen als Sicherheitsmaßnahme offensichtlich nicht aus.

Maßnahmen in einem Mitgliedstaat können im **Schutzklauselverfahren** auf den gesamten Binnenmarkt erstreckt werden (Art. 66 Abs. 2 KI-VO-E). 71

C. Code of Conduct

Nach Art. 69 KI-VO-E ist für Betreiber solcher KI-Systeme, welche nicht der Kategorie der hochriskanten Anwendungen unterfallen, die Möglichkeit eröffnet, sich einem freiwilligen **Verhaltenskodex** (Code of Conduct) zu unterwerfen. Die Vorschrift gilt für Systeme „ohne besondere Risiken" wie auch für Systeme mittlerer Risikokategorie.[87] Freiwillige Verhaltenskodizes sind aus vielen Branchen bekannt, etwa aus der Werbe- und Zigarettenindustrie oder aus der Lebensmittel- und Arzneimittelindustrie etc. Dieses Regulierungsinstrument hat man auf europäischer Ebene schon wiederholt bemüht – nicht nur in Art. 40 DS-GVO ist es zu finden,[88] sondern auch in der VO (EU) 2019/1150 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten. 72

Der europäische Gesetzgeber misst demnach der Selbstregulierung der Wirtschaft offensichtlich eine hohe Bedeutung bei und er setzt darauf, dass die Marktstandards mittels **„Soft Law"** stetig angehoben werden. In der Praxis werden die freiwilligen Kodizes formuliert, um den eigenen Unternehmensangehörigen konkrete Handlungshilfen an die Hand zu geben.[89] In Haftungsprozessen können sie relevant werden, um dem Vorwurf eines Organisationsverschuldens zu begegnen und sie können helfen, die Einhaltung von etwaigen Aufsichtspflichten nachzuweisen.[90] Von den Verwendern werden freiwillige Kodizes bisweilen auch wegen eines **positiven Reputationseffekts** aufgegriffen. 73

Marktteilnehmer können sich gem. Art. 69 Abs. 1 KI-VO-E freiwillig dafür entscheiden, das strikte Complianceprogramm, wie es aus Titel III Kapitel 2 des KI-VO-E folgt, auf Systeme mittlerer oder niedriger Kritikalität teilweise oder vollständig[91] zu übertragen. Diese Kodizes sollen bestenfalls nicht nur die Vorgaben des KI-VO-E aufgreifen, sondern auch weitere ökologische und gesellschaftliche Standards abbilden – jeweils „to the best extent possible".[92] Der Kommission, den Mitgliedstaaten und dem Ausschuss ist gesetzlich diesbzgl. eine Unterstützungs- und **Förderpflicht** auferlegt (Art. 69 Abs. 1, 2 KI-VO-E). Den besonderen Bedürfnissen von Kleinanbietern und Startups ist gem. Art. 69 Abs. 4 KI-VO-E ausreichend Rechnung zu tragen. 74

Für Marktteilnehmer wichtig ist die aus Art. 69 Abs. 3 KI-VO-E (mittelbar) folgende Einschränkung: es gibt nicht „den einen Standard". Der Anbieter kann eigene Standards entwickeln, insbes. um (aus Reputationsgründen) die individuellen Wertvorstellungen und das Selbstverständnis nach außen erkennbar zu verschriftlichen; er kann aber auch bestehende, insbes. **verbandsweite Complianceanforderungen** aufgreifen, diese auf eigene Bedürfnisse wiederum anpassen etc. 75

Welche Effektivität die Kodizes in der Praxis tatsächlich haben, ist abstrakt schwierig zu bestimmen. Von einer nicht zu unterschätzenden Relevanz sind sie sicherlich dort, wo die branchenbezogenen Verhaltensstandards zentralistisch von einem Verband kommuniziert werden; dies zeigt bspw. der Bankensektor. Ein eigensinnig agierendes Verbandsmitglied 76

[87] Enger wohl Bomhard/Merkle RDi 2021, 276 Rn. 37: für Systeme „ohne besonderes Risiko"; enger auch Rostalski/Weiss ZfDR 2021, 329 (353).
[88] S. zu verschiedenen Aspekten und Auswirkungen der Kodizes im Danteschutzrecht ua Reifert ZD 2019, 305; Wittmann/Haidenthaler MMR 2022, 8.
[89] Kramer IT-ArbR/Schulze-Zumkley B Rn. 1153.
[90] Kramer IT-ArbR/Schulze-Zumkley B Rn. 1153.
[91] Diese Einschränkung wird im Kompromisstext betont, vgl. Art. 69 Abs. 1 Ratsdok. 11124/22.
[92] Im Kompromisstext ist dies für Art. 69 Abs. 1, nicht aber für Abs. 2 klargestellt, vgl. Ratsdok. 11124/22.

wird seinen Kunden schwerlich erklären können, weshalb es einen weithin anerkannten Branchenstandard nicht befolgen will. Zudem wäre mit einer solchen Abweichung ein nicht unerhebliches Prozessrisiko verbunden, denn die Gerichte messen eine Bankenmaßnahme im Schadensfall für den Kunden typischerweise am in der Branche geltenden Standard. Abweichungen sind dementsprechend in diesem Sektor die Ausnahme.

77 An der Effizienz der nach Art. 69 KI-VO-E begünstigten Kodizes lässt sich aus drei Gründen gleichwohl zweifeln: *Erstens* fehlt die spezifische Sanktionierung von Verstößen, jedenfalls so lange die Complianceanforderungen noch nicht in Form von Verkehrssicherungspflichten etc. zu materiellrechtlich verbindlichen Pflichten geronnen sind. *Zweitens* ist keine zielgerichtete Belohnung für die Befolgung des Kodex vorgesehen; selbst aus der DS-GVO bekannte Nachweiserleichterungen[93] sind für die Kodizes nach Art. 69 KI-VO-E (bisher) nicht vorgesehen.[94] *Drittens* dienen die freiwilligen Verhaltensregeln in der Regel der Präzisierung unbestimmter, generalklauselartiger Normen des materiellen Rechts,[95] während es bei den in Art. 69 KI-VO-E angesprochenen Kodizes noch an den Anknüpfungspunkten für eine Präzisierung fehlt; dies kann ein erheblicher Unsicherheitsfaktor für Anbieter sein.

[93] S. beispielhaft Art. 24 Abs. 3 DS-GVO, Art. 28 Abs. 5 DS-GVO, Art. 32 Abs. 3 DS-GVO.
[94] Krit. insoweit auch Spindler CR 2021, 261 Rn. 71; Rostalski/Weiss ZfDR 2021, 329 (353).
[95] S. dazu etwa BeckOK DatenschutzR/Jungkind DS-GVO Art. 40 Rn. 3.

§ 8. Konformitätsbewertungsverfahren, Organisation und Mittel der KI-Aufsichtsbehörden und Europäischer KI-Ausschuss

Im Wesentlichen setzt der KI-VO-E zur Umsetzung seiner Pflichten auf eine Selbstregulierung der beteiligten Wirtschaftsakteure. Subsidiär wird diese Selbstregulierung mit einem verwaltungsrechtlichen Überbau ergänzt, der insbes. bei (ex-ante) Konformitätsbewertung und (ex-post) Marktüberwachung zur Anwendung kommt. Während die Verwaltung in der Konformitätsbewertung auch bei Hochrisikosystemen auf Einzelfälle beschränkt erscheint, da der Grundsatz der Konformitätsbewertung auf Basis einer anbieterinternen Kontrolle nach Art. 43 Abs. 2 KI-VO-E iVm Anhang VI KI-VO-E gilt (vgl. auch → § 7 Rn. 10), tritt sie in der Marktüberwachung zentral in Erscheinung. Dieser Abschnitt widmet sich dem Verwaltungsrecht der KI, insbes. dem verwaltungsverfahrens- und organisationsrechtlichen Teil der KI-Verordnung und dem zentralen Aspekt der Sanktionen für Fehlverhalten. Dabei ist die Konformitätsbewertung durch notifizierte Stellen (A.), die aufsichtsrechtliche Behandlung nach dem Inverkehrbringen (B.), die Organisation der nationalen KI-Behörden (C.) und der Europäische KI-Ausschuss (D.) zu besprechen. Der Beitrag schließt mit einer vorläufigen Bewertung der genannten Aspekte im Entwurf (E.), die im noch laufenden Gesetzgebungsverfahren intensiv diskutiert werden. 1

A. Die Konformitätsbewertung durch notifizierte Stellen

Im Gesamtzusammenhang der KI-Verordnung stellt die **Fremdzertifizierung von KI-Systemen durch Verwaltungsbehörden** eine **Ausnahme** dar.[1] Art. 43 Abs. 2 KI-VO-E verweist auf Anhang III Nr. 2–8 KI-VO-E und statuiert für die dort aufgeführten Fälle das Prinzip der Selbstzertifizierung auf Grundlage einer internen Kontrolle. Dies gilt etwa für Hochrisikosysteme, die für die Verwaltung und den Betrieb kritischer Infrastrukturen eingesetzt werden, für allgemeine und berufliche Bildung, für Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit, für Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen, Strafverfolgung, für Migration, Asyl und Grenzkontrolle sowie für Rechtspflege und demokratische Prozesse mit all den von Anhang III KI-VO-E vorgesehen detaillierten Anwendungsbeispielen. 2

Die **Konformitätsbewertung durch notifizierte Stellen** gem. Anhang VII KI-VO-E ist gegenwärtig nur nach Art. 43 Abs. 1 KI-VO-E iVm Anhang III Nr. 1 KI-VO-E für Systeme vorgesehen, die der biometrischen Identifizierung und Kategorisierung natürlicher Personen dienen, insbes. (Buchst. a) KI-Systemen, die bestimmungsgemäß für die biometrische Fernidentifizierung verwendet werden sollen.[2] Verpflichtend ist sie dort nur, solange es noch keine harmonisierten Normen oder Spezifikationen nach Art. 40 bzw. Art. 41 KI-VO-E gibt.[3] Ausnahmen sind ferner nach Art. 43 Abs. 3 KI-VO-E solche KI-Systeme, die unter spezielle Produktsicherheitsrechtsakte fallen (zB VO (EU) 2017/745 „Medizinprodukte-VO"), die eigene notifizierte Stellen aufweisen. Hier sind zur Vermeidung unnötigen Verwaltungsaufwands die dortigen Stellen zuständig,[4] wobei bestimmte Verfahrensaspekte des Anhangs VII KI-VO-E Eingang in die Konformitätsbewertung finden (→ Rn. 7 zur Bewertung der technischen Dokumentation). Für KI-Systeme, die von Finanzinstituten in Betrieb genommen werden, gilt das 3

[1] Dazu auch Spindler CR 2021, 361 (370) sowie Roth-Isigkeit ZRP 2022, 187 (188).
[2] Dazu auch Erwgr. Nr. 8 KI-VO-E.
[3] Die besondere Rolle dieser Standards betont Spindler CR 2021, 361 (369).
[4] S. Erwgr. Nr. 63 KI-VO-E; vgl. ferner Begr. Nr. 1.2 KI-VO-E.

Verfahren der Beaufsichtigung von Kreditinstituten nach Art. 97 ff. RL 2013/36/EU („CRD IV").

4 Dies wirkt zunächst wie ein sehr schmaler Anwendungsbereich für das Verfahren nach Anhang VII KI-VO-E.[5] Zu beachten ist jedoch, dass der **Kommission** nach Art. 43 Abs. 6 KI-VO-E die **Befugnis** übertragen werden soll, mit **delegiertem Rechtsakt** die in Anhang III Nr. 28 KI-VO-E genannten Anwendungen doch dem formalisierten Konformitätsbewertungsverfahren durch notifizierte Stellen zu unterwerfen. Insoweit kann das Verfahren potentiell zentrale Bedeutung erlangen. Zum gegenwärtigen Stand will die Kommission insbes. die Überlastung von Aufsichtsbehörden vermeiden.[6]

I. Das Verfahren nach Anhang VII KI-VO-E

5 Der Anbieter hat zunächst nach Art. 43 Abs. 1 UAbs. 3 KI-VO-E grds. die **freie Wahl der notifizierten Stelle,** bei der er das Verfahren durchführen will. Der etwas unsystematisch im vorderen Teil der Verordnung befindliche Art. 23 KI-VO-E verlangt von Anbietern von KI-Systemen eine **intensive Zusammenarbeit mit den Aufsichtsbehörden.** Diese übermitteln den nationalen Behörden auf deren Verlangen „alle Informationen und Unterlagen, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems […] nachzuweisen." Soweit dies erforderlich ist, gehören dazu auch die vom KI-System automatisch erzeugten Protokolle, falls diese dem Anbieter selbst zur Verfügung stehen. Anhang VII KI-VO-E regelt sodann das anwendbare Konformitätsbewertungsverfahren auf der Grundlage der Bewertung des Qualitätsmanagementsystems (QMS) und der Bewertung der technischen Dokumentation.[7] Nach Art. 43 Abs. 5 KI-VO-E iVm Art. 73 KI-VO-E kann die Kommission delegierte Rechtsakte zur Anpassung des Konformitätsbewertungsverfahrens an den technischen Fortschritt erlassen, hier ist also eine gewisse **Flexibilität** zu erwarten.

6 Grundlage des QMS für die Konzeption, Entwicklung und das Testen von KI-Systemen ist der **Antrag des Anbieters** bei der notifizierten Stelle. Dieser muss die in Anhang VII Nr. 3.1 KI-VO-E genannten Daten umfassen. Dazu zählen neben Namen und Anschrift des Anbieters, bzw. bei Antragstellung durch Bevollmächtigten zusätzlich auch dessen Name und Anschrift (Buchst. a), die Liste der unter dasselbe QMS fallenden KI-Systeme (Buchst. b), die technische Dokumentation für jedes unter dasselbe QMS fallende KI-System (Buchst. c), die Dokumentation über das QMS mit allen Aspekten des Art. 17 KI-VO-E (Buchst. d) auch eine Beschreibung der bestehenden Verfahren, mit denen sichergestellt wird, dass das QMS geeignet ist und auch in Zukunft wirksam bleibt (Buchst. e), sowie eine schriftliche Erklärung, dass der Antrag bei keiner anderen notifizierten Stelle eingereicht worden ist (Buchst. f). Auf Grundlage dieses Antrags bewertet die notifizierte Stelle, ob die Anforderungen des Art. 17 KI-VO-E erfüllt sind. Wird dies bejaht, genehmigt die notifizierte Stelle das QMS. Die Ergebnisse der Bewertung und die begründete Bewertungsentscheidung teilt sie dem Anbieter oder dessen Bevollmächtigten mit (Anhang VII Nr. 3.2 KI-VO-E).

7 Neben dem Antrag auf Genehmigung des QMS stellt der Anbieter auch einen Antrag auf **Bewertung der technischen Dokumentation** für das KI-System (Anhang VII Nr. 4 KI-VO-E) bei der notifizierten Stelle. Im Rahmen dieses Bewertungsverfahrens erhält die notifizierte Stelle **uneingeschränkten Zugang** zu den vom Anbieter verwendeten **Trai-**

[5] So auch empfohlen im Gutachten der Datenethikkommission vom 23.10.2019, 201, abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html;jsessionid=FF71C19934371EB93FE4A14E4C67E962.1_cid334?nn=11678504 (zuletzt aufgerufen am 4.10.2022).

[6] Dies geht aus der Verordnungsbegründung hervor, vgl. Begr. Nr. 5.2.3 KI-VO-E.

[7] Dies entspricht der High Level Expert Group on AI, Policy and Investment Recommendations for Trustworthy AI, Empfehlung 29.4, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence (zuletzt aufgerufen am 4.10.2022).